КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (10), 2020
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2020.10.158168
УДК 004.94:519.21

Шевченко Світлана Миколаївна
Канд. пед. наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки
Київський університет імені Бориса Грінченка, м. Київ, Україна
ORCID: 0000-0002-9736-8623
S.shevchenko@kubg.edu.ua

Жданова Юлія Дмитрівна
Канд. ф.-м. наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки
Київський університет імені Бориса Грінченка, м. Київ, Україна
ORCID: 0000-0002-9277-4972
Y.zhdanova@kubg.edu.ua

Спасітєлєва Світлана Олексіївна
Канд. ф.-м. наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки
Київський університет імені Бориса Грінченка, м. Київ, Україна
ORCID: 0000-0003-4993-6355
S.spasitielieva@kubg.edu.ua

Складанний Павло Миколайович
Старший викладач кафедри інформаційної та кібернетичної безпеки
Київський університет імені Бориса Грінченка, Київ, Україна
ORCID: 0000-0002-7775-6039
P.skladannyi@kubg.edu.ua

ПРОВЕДЕННЯ SWOT-АНАЛІЗУ ОЦІНЮВАННЯ ІНФОРМАЦІЙНИХ РИЗИКІВ ЯК ЗАСІБ ФОРМУВАННЯ ПРАКТИЧНИХ НАВИЧОК СТУДЕНТІВ СПЕЦІАЛЬНОСТІ 125 КІБЕРБЕЗПЕКА

Анотація. В даній статті розглядається проблема впровадження активних методів навчання студентів спеціальності 125 Кібербезпека. На прикладі вивчення дисципліни «Теорія ризиків» представлено дослідження якісного аналізу ризиків інформаційної безпеки (ІБ), а саме, застосування інструментарію SWOT-аналізу для оцінювання ризиків у сфері ІБ малого та середнього бізнесу. Обґрунтовано актуальність та можливості використання SWOT-аналізу в сфері ризикології ІБ для вивчення внутрішнього середовища організації, її сильних і слабких сторін з метою визначення стратегії підприємства у зовнішньому середовищі: протистояння загрозам безпеці інформації (порушення конфіденційності, доступності та цілісності), а також використання зовнішніх можливостей для свого розвитку. Спираючись на наукові джерела, проаналізовані основні дефініції дослідження: ризики ІБ, аналіз ризиків та їх якісне оцінювання. Описано зміст і процедуру проведення SWOT-аналізу.
Використовуючи форми групової роботи та активні методи (тренінги) у навчальному процесі, було створено базу факторів для SWOT-аналізу віртуальної організації «Інтернет-провайдер», проведено метод експертних оцінок для виставлення першочерговості цих факторів, здійснено аналіз отриманих результатів.
Доведено, що впровадження даної технології у навчальний процес сприяє ефективному засвоєнню теоретичних знань та формуванню і розвитку практичних навичок майбутніх фахівців інформаційної та кібернетичної безпеки.

Ключові слова: ризики інформаційної безпеки; аналіз ризиків; SWOT-аналіз; загрози; активні методи навчання.

1. ВСТУП

Постановка проблеми. Динамічний розвиток інформаційних технологій вимагає від фахівців інформаційної безпеки сучасних знань та практичних навичок. У «Звіті про майбутнє робочих місць за 2020 рік» [1] наголошується, що саме на спеціалістів-аналітиків ІБ попит у роботодавців зростає. Цьому сприяє прискорення автоматизації процесів та збільшення ризиків кібербезпеки. Дане опитування [1] дозволило виділити двадцять найбільш затребуваних спеціальностей, серед яких Information Security Analysis (8 місце) та Risk Management Specialists (20 місце). Автори звіту виділили необхідні навички для успішної кар'єри, серед яких аналітичне мислення та інноваційність; активне навчання і навчальні стратегії; комплексне розв'язання проблеми; критичне мислення й аналіз; креативність, оригінальність та ініціативність; лідерство і соціальний вплив. Є очевидним, що перед вищою школою стоять завдання по організації навчального процесу з метою ефективного формування цих навичок у процесі вивчення дисциплін. А з точки зору психології, саме вік 19-25 є найбільш сприятливим для розвитку цих навичок [2].

Аналіз останніх досліджень і публікацій. Велика кількість сучасних наукових досліджень з проблеми формування практичних навичок студентів, зокрема спеціальності 125 Кібербезпека, свідчить про важливість даного питання [3] – [11]. Вченими пропонуються різні шляхи розвитку практичної складової студентства: впровадження віртуальних лабораторій [4], [7], [8], [10]; запровадження активних форм і методів навчальної діяльності [5], [6], [9]; організація науково-дослідної роботи [11] та інші. Проте в одному вони одностайні: найкращі теоретичні знання не в змозі дати те, що дає особистий досвід власної діяльності. Тому значення набувають у ЗВО ті форми, засоби та методи навчальної діяльності, які активізують мислення, стимулюють до творчості, адаптують до професійної діяльності. Особливо тепер, в умовах скорочення робочих місць у зв'язку з пандемією та модернізацією технологічних процесів.

Висвітлені проблеми дають переконливе уявлення про актуальність даного дослідження і визначають його мету.

Мета статті. Метою статті є представлення методики формування практичних навичок якісного оцінювання ризиків ІБ за допомогою SWOT-аналізу у студентів спеціальності 125 Кібербезпека.

2. ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Практика впровадження ризик-менеджменту в інформаційну безпеку організації показала, що існують різні представлення даного процесу. У зв'язку з цим є потреба здійснити огляд понять і підходів до сфери ризикології ІБ у науковій літературі та нормативних документах.

До середини XX ст. Ризики вивчались, аналізувались та оцінювались, головним чином, для економічної системи, в областях економічної теорії (проблеми страхування, інвестування, розвитку бізнесу та ін.). Однак, у другій половині XX ст. Виявилось, що

методологія оцінки ризиків може бути впроваджена в аналіз та в забезпечення безпеки практично будь-якої системи (соціальної, технічної, біологічної, екологічної та ін.). Бурхливі темпи створення нових інформаційно-комунікаційних технологій, зростання обсягів цифрової інформації і підвищення її значимості несуть у собі ризики, потенційно створюють передумови для витоку, розкрадання, втрати, спотворення, підробки, знищення, копіювання і блокування інформації і, як наслідок, ведуть до заподіяння шкоди. Інформаційні ризики посіли одне з центральних місць в теорії ризикології. А в якості системної методології захисту інформації стали використовувати підхід оцінювання та управління інформаційними ризиками.

Аналіз наукових джерел [12] – [17] дозволив виділити, що

- Однозначного трактування поняття «ризик ІБ» не існує;
- Ототожнюють поняття «ризик інформаційний» та «ризик інформаційної безпеки»;
- «ризик ІБ» використовують лише тоді, коли існує можливість негативних наслідків;
- «ризик ІБ» розглядають як комбінацію ймовірності події та її наслідку;
- Поняття «ризик ІБ» є комбінованим, який поєднує в собі інші ключові терміни (активи, уразливості, загрози, збиток).

Враховуючи всі перераховані фактори, вважаємо, що ризик інформаційної безпеки – це числова (словесна) функція, яка описує ймовірність втілення загроз ІБ та величини збитку від їх реалізації внаслідок використання цими загрозами уразливостей активів з метою нанесення шкоди організації.

Під управлінням ризиками ІБ (ризик-менеджмент) розуміють безперервний циклічний процес, який містить наступні етапи: ідентифікація ризиків (збір інформації щодо активів, джерел загроз, класифікація загроз та уразливостей; ранжування ризиків); аналіз ризику (якісний та кількісний підхід до оцінки ризику); оцінювання ризику (процес порівняння кількісно оціненого ризику з даними критеріями ризику для визначення значущості ризику ІБ); обробка ризику та прийняття. На рисунку 1 представлено алгоритм процесу управління ризиками ІБ [15].

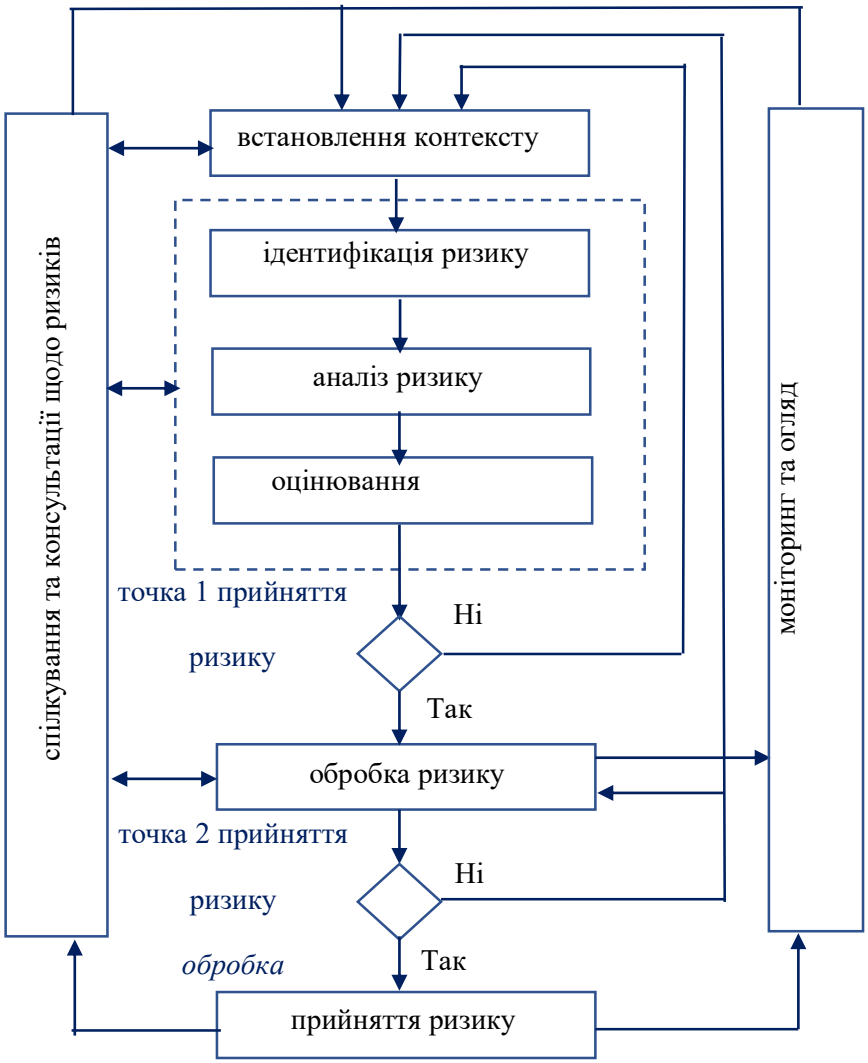

Рис. 1. Алгоритм процесу ризиками ІБ

Ефективність обробки ризиків ІБ істотно залежить від оцінки цих ризиків. Розрізняють якісний та кількісний підхід до встановлення значень ризиків ІБ.

Якісний підхід до кількісної оцінки ризиків ІБ використовує словесну шкалу можливих наслідків (низька, середня та висока) та ймовірність виникнення даних наслідків. Переваги: зрозумілість всьому персоналу; недоліки: суб'єктивність такого вибору. Такий підхід застосовується:

- Як початковий при ідентифікації ризиків ІБ, які надалі будуть проаналізовані більш детально;
- Коли достатньо такого аналізу для прийняття рішення;
- Коли числових даних або ресурсів для кількісної оцінки недостатньо.

Якісний аналіз використовує фактичну інформацію та дані.

Кількісний підхід до кількісної оцінки ризиків ІБ використовує шкалу з числовими значеннями як для наслідків так і для ймовірностей, ґрунтуючись на даних, отриманих із різних джерел. Переваги: безпосередній зв'язок з задачами та потребами організації в ІБ, бо він використовує фактичні дані за попередній період про інциденти ІБ; недоліки: відсутність даних по новим ризикам ІБ та уразливості.

Наше дослідження присвячено якісному підходу в оцінці ризику, тому зупинимося на інструментарії цього підходу, а саме SWOT-аналізу.

Аналіз-SWOT- дослідницька процедура, ідея якої полягає в комплексному описі сил (Strength), слабкостей (Weakness), можливостей (Opportunities), загроз (Threats) при розробці стратегії організації. Зміст цієї процедури такий:

А) вивчаються сили - конкурентні переваги організації на певних ділянках;

Б) вивчаються слабкості - негативні внутрішні чинники;

В) вивчаються політичні, економічні, технологічні, соціальні фактори макросередовища організації з метою виявлення стратегічних і тактичних загроз та своєчасного попередження збитків від них;

Г) вивчаються стратегічні й тактичні можливості організації, необхідні для зменшення “слабкостей” і зміцнення “сил”;

Д) сили погоджуються з можливостями для формування нової стратегії [18, с.107].

Оформляється дана технологія у вигляді матриці, яка представлена в таблиці 1, а рішення – в таблиці 2.

Таблиця 1

SWOT-аналіз

Strength	Weakness
S1.	W1.
S2.	W2.
Opportunities	Threats
O1.	T1.
O2.	T2.
O3.	T3.

Таблиця 2

SWOT-матриця стратегічних рішень

	Threats (T)	Opportunities (O)
Strength (S)	Максимізація сильних сторін для протистояння загрозам ST	Максимізація сильних сторін для використання можливостей зовнішнього середовища SO
Weakness (W)	Мінімізація впливу слабких сторін та уникнення загрози WT	Мінімізація впливу слабких сторін внаслідок можливостей зовнішнього середовища WO

Як свідчить аналіз літератури, історія розвитку технології SWOT є суперечливою [19]. Вважають, що SWOT-аналіз створений двома професорами відділу політики Гарвардської школи бізнесу Джорджу Альберту Сміту-молодшому та С. Роланду Крістенсену на початку 1950 років. Пізніше професор Кеннет Ендрюс вдосконалив цю технологію і впровадив для використання. Всі професори були спеціалістами не маркетингу, а в області організаційної стратегії. Проте, як стверджує автор [19],

задокументованої історичної довідки витоків SWOT-аналізу не існує. Слід відмітити, що Шинно Х. Та його колеги (2006 рік) об'єднали дану технологію з процесом аналітичної ієрархії, що дозволило ранжувати елементи за допомогою програмного забезпечення.

Метод SWOT-аналізу є універсальним і одночасно нескладним методом стратегічного дослідження діяльності підприємств, що дозволило його застосувати для якісного підходу оцінювання ризиків ІБ [20], [21].

3. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

3.1. Постановка завдання

У процесі вивчення дисципліни «Теорія ризиків» на практичному занятті студентам 3 курсу спеціальності 125 Кібербезпека Київського університету імені Бориса Грінченка було запропоновано здійснити SWOT-аналіз ризиків ІБ організації за вибором, сфера діяльності якої більш-менш є зрозумілою (робота батьків, практика, власна діяльність та інше). На минулих лекціях зі студентами обговорювалися зміст та процедура проведення SWOT-аналізу підприємства. Як домашнє завдання, потрібно було проаналізувати наукові джерела щодо впровадження даної технології для аналізу та вироблення стратегії підприємства в будь-якій галузі.

Форму навчання обрали групову, що дозволило розподілити студентів на аналітиків, відповідальних за ІБ в своїй організації, та експертів, які оцінювали фактори з власної точки зору, спираючись на праці науковців, статистичні дані та інше.

Найбільш доцільним для формування фахових практичних навичок, на нашу думку, навчальний процес студентів представити у вигляді тренінга. Саме тренінг орієнтований на запитання та пошук відповіді, саме під час тренінгу створюється неформальне невимушене спілкування, яке розкриває перед групою можливість висловити свою точку зору та обґрунтувати її.

3.2. Формування факторів в матриці SWOT-аналізу

Між студентами була узгодженість здійснити SWOT-аналіз ризиків ІБ віртуальної організації «Інтернет-провайдер».

В результаті обговорення було визначено активи фірми, джерела загроз ІБ, класифікація загроз та уразливостей. На основі даних сформульовані фактори, які представлені в таблиці 3.

Таблиця 3

SWOT-аналіз ризиків ІБ організації «Інтернет-провайдер»

Strength	Weakness
S1. Висококваліфікований персонал	W1. Відсутність системи аварійного електропостачання
S2. Сертифіковані засоби захисту інформації	W2. Відсутність системи регулярного резервного копіювання
	W3. Відсутність двофакторної аутентифікації
Opportunities	Threats
O1.Закупка нового обладнання	T1. Витік інформації
O2.Налагодження взаємодії з бізнес-партнерами, інвесторами	T2. Підкуп персоналу
	T3. Зміна нормативної бази в сфері ІБ

3.3. Створення експертної групи та побудова експертних оцінок

Методи експертних оцінок – це способи оцінювання, засновані на використанні знань, досвіду та інтуїції фахівців-експертів. Застосовується як індивідуальна, так і колективна експертиза. Найпростішими методами індивідуальних експертних оцінок є: анкетування, інтерв'ювання, розроблення аналітичних оглядів за визначеними проблемами. Перевагами цих методів є взаємна незалежність думок експертів, мінімізація конформізму, можливість формалізації процедур збору та обробки даних. Серед методів колективної експертизи виділяють методи на зразок «Комісії», «Мозкового штурму», «Дельфі». При проведенні колективної експертизи робиться припущення, що істинне значення досліджуваної характеристики перебуває в середині діапазону оцінок експертів і що узагальнена думка експертів є достовірною. Перевагою методу є більш висока надійність результату за рахунок узагальнення колективної думки, а недоліком – можливість взаємного впливу експертів, їх психологічна несумісність тощо [18, с.117].

Автори [22] представили широкий аналіз експертних оцінок, включаючи і процедуру формування експертної групи, методи оцінювання компетентності представників експертної групи, основні переваги та недоліки індивідуальних та колективних методів, оцінювання ступеня погодженості суджень групи експертів та їх статистичної ймовірності.

Враховуючи максимально вимоги до створення експертної групи, формуємо її. Кожний експерт досліджує дану проблему та відповідний вплив факторів.

Створюється таблиця експертних оцінок по кожному критерію (наприклад, по критерію – слабкі сторони). Дані представлені в таблиці 4.

Таблиця 4

Зважені оцінки факторів слабких сторін організації

Weakness	Ступінь Важливості	Вагомий коефіцієнт	Експертні оцінки					Середня оцінка	Зважена оцінка
W1. Відсутність системи аварійного електропостачання	2	0,33	5	3	5	3	4	4	4x0,33=1,32
W2. Відсутність системи регулярного резервного копіювання	3	0,5	3	3	3	3	3	3	3x0,5=1,5
W3. Відсутність двофакторної аутентифікації	1	0,17	2	4	4	3	3	4	4x0,17=0,68
Всього	6	1							3,5

Аналогічно здійснюється експертна оцінка для кожного критерію матриці SWOT-аналізу.

Наступним кроком є створення інтерактивних матриць для рангової оцінки між зовнішніми загрозами та внутрішніми слабкими сторонами; між можливостями та внутрішніми сильними сторонами (таблиця 5).

Таблиця 5

Інтерактивна матриця для рангової оцінки між зовнішніми загрозами та внутрішніми слабкими сторонами організації

	W1	W2	W3
T1	+	+	+
T2	+	+	0
T3	0	0	+

Пріоритетною є та загроза, яка має найбільше поєднань з слабкими сторонами організації (у нашому прикладі це T1).

3.4. Зведення результатів та їх аналіз

Заповнення чотирьох квадрантів на перетині сильних/слабких сторін, можливостей/загроз дозволять виявити та описати чотири види стратегії: SO – пвизначаються орієнтири стратегічного розвитку організації; ST – визначаються потенційні стратегічні переваги компанії; WO – визначаються орієнтири внутрішніх перетворень організації; WT – фіксуються обмеження стратегічного розвитку. Наприклад, SO1 – вихід на нові території та розширення клієнтської бази; WO2 – створення системи аварійного електропостачання; ST2 – преміювання персоналу та створення більш комфортних умов для праці; WT1 – моніторинг системи резервного копіювання.

4. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Вивчення кожної дисципліни студентами у вищій школі потрібно розглядати як відповідну сходинку у процесі саморозвитку, як етап у формуванні конкурентоспроможного фахівця інформаційної та кібернетичної безпеки. Впровадження у навчальний процес ЗВО активних форм навчання, зокрема тренінгів, сприяє формуванню практичних навичок, що дозволяє адаптувати наших студентів до професійної діяльності у майбутньому.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] The Future of Jobs Report 2020. [Онлайн] Режим доступу: https://www.weforum.org/reports/the-future-of-jobs-report-2020

[2] С.М. Шевченко С.М. Розвиток аналітичного мислення студентів вищих технічних навчальних закладів у процесі вивчення математичних дисциплін.- Дисертація канд. Пед. Наук: 13.00.02, Нац. Пед. Ун-т ім. М. П. Драгоманова. - К., 2013.- 200 с.

[3] *Освітньо-професійна програма. 125.00.01. Безпека інформаційних і комунікаційних систем першого (бакалаврського) рівня освіти.* Київський університет імені Б. Грінченка, 2018. [Онлайн] Режим доступу: http://kubg.edu.ua/images/stories/Departaments/vstupnikam/fitu/2018/2019_bak_op_kiber.pdf

[4] В.Л. Бурячок, В.М. Богуш, Ю.В. Борсуковський, П.М. Складанний, В.Ю. Борсуковська, "Модель підготовки фахівців у сфері інформаційної та кібернетичної безпеки в закладах вищої освіти України", *Інформаційні технології і засоби навчання,* том 67, №5, с.277-289, 2018.

[5] Бурячок В.Л., Богуш В.М. (2018) *Рекомендації щодо розробки та реалізації моделі професійних компетентностей у сфері підготовки фахівців для національної системи кібербезпеки* Захист інформації, Т.20 (2). С. 72-78. ISSN 2221-5212

[6] Мельник С., Воскобойніков С., Ступак Д. Організація фахової підготовки майбутніх фахівців з кібербезпеки на основі інноваційної педагогіки та інтегрованого підходу в системі реалізації ключових компетенцій безпеки в інформаційному суспільстві. *Витоки педагогічної майстерності, вип. 21, 2018, с.125 - 129*

[7] V. L. Buriachok, S. M. Shevchenko, і P. M. Skladannyi, «Віртуальна лабораторія для моделювання процесів в інформаційній та кібербезпеці як засіб формування практичних навичок студентів», *Кібербезпека: освіта, наука, техніка*, вип. 2, вип. 2, с. 98-104, Груд 2018.

[8] Ю.Д. Жданова, С.О. Спасітєлєва, С.М. Шевченко, "Застосування бібліотеки класів Security.Cryptography для практичної підготовки спеціалістів з кібербезпеки", *Кібербезпека: освіта, наука, техніка*, 4(4), с. 44-53, 2019.

[9] Buriachok, Volodymyr и Sokolov, V. Y. (2019) *Implementation of Active Learning in the Master's Program on Cybersecurity* In: II International Conference on Computer Science, Engineering and Education Applications (ICCSEEA'2019), 26,27 January 2019, Kyiv.

[10] V. Buriachok, N. Korshun, S. Shevchenko, і P. Skladannyi, «Застосування середовища ni multisim при формуванні практичних навичок студентів спеціальності 125 'кібербезпека'», *Кібербезпека: освіта, наука, техніка*, вип. 1, вип. 9, с. 159-169, Вер 2020.

[11] Шевченко С.М., Жданова Ю. Д., Спасітєлєва С. О., Адамович О. В. Статистична обробка експериментальних даних як одна з форм науково-дослідної роботи студентів спеціальності «Кібербезпека» *Сучасний захист інформації №2(30), 2017, с. 95-103*

[12] «Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology [Gary Stoneburner, Alice Goguen, Alexis Feringa]», National Institute of Standards and Technology Special Publication 800- 30, Falls Church: Natl. Inst. Stand. Technol, 2002, p. 54

[13] «Risk analysis based on IT-Grundschutz», BSI-Standard 100-3, Boon: Bundesamt für Sicherheit in der Informationstechnik, 2008, p. 23

[14] «Information Technology – Security techniques – Information security risk management (ISO/IEC 27005:2008)», ISO/IEC JTC 1/SC 27, 2008, p. 62.

[15] ДСТУ ISO/IEC 27005:2019 (ISO/IEC 27005:2018, ІДТ) «Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки», 2019, с. 54

[16] Архипов О.Є., Муратов О.Є., Бровко В.Д. Основи теорії ризиків: навчальний посібник – К.: НА СБ України, 2019. – 267 с.

[17] Ахметов Б.Б., Корченко А.Г., Архипов А.Е., Казмирчук С.В. Построение систем анализа и оценивания рисков информационной безопасности. Теория и практические решения: монография (в 2-х книгах) – Актау: редакционно-издательский отдел КГУТИ им. Ш. Есенова, 2018. – 390 с. (кн. 1), 346 с. (кн. 2). [Онлайн] Режим доступу: https://er.nau.edu.ua/handle/nau/40479?locale=uk

[18] Словник системного аналізу в державному управлінні. К., 2006, с.148. [Онлайн] Режим доступу: http://academy.gov.ua/nmkd/library_nadu/encycloped_vydanniy/f4a14404-2b5a-4031-968c-c95c5a50b4c5.pdf

[19] Tim Friesner. History of SWOT Analysis, 2011. [Онлайн] Режим доступу: https://www.marketingteacher.com/history-of-swot-analysis/

[20] Andrea Berkoff Security SWOT Analysis for 2020: Opportunities, 2020. [Онлайн] Режим доступу: https://citysecuritymagazine.com/risk-management/security-sector-leaders-swot-analysis-for-2020-opportunities/

[21] Scholarly Commons Citation Baghdasarin, D. (2019). MRO Cybersecurity SWOT. International Journal of Aviation, Aeronautics, and Aerospace, 6(1). https://doi.org/10.15394/ijaaa.2019.1318

[22] Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. Ред. Д-ра техн. Наук, професора В. Б. Толубка.— К.: ДУТ, 2015.— 288 с.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (10), 2020
ISSN 2663 - 4023

Svitlana M. Shevchenko
PhD, Associate Professor, Associate Professor of the Department of Information and Cyber Security
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID: 0000-0002-9736-8623
s.shevchenko@kubg.edu.ua

Yuliia D. Zhdanova
PhD, Associate Professor, Associate Professor of the Department of Information and Cyber Security
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID: 0000-0002-9277-4972
y.zhdanova@kubg.edu.ua

Svitlana O. Spasiteleva
PhD, Associate Professor, Associate Professor of the Department of Information and Cyber Security
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID: 0000-0003-4993-6355
s.spasitielieva@kubg.edu.ua

Pavlo M. Skladannyi
Senior Lecturer of the Department ofinformation and Cyber Security
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID: 0000-0002-7775-6039
p.skladannyi@kubg.edu.ua

CONDUCTING A SWOT-ANALYSIS OF INFORMATION RISK ASSESSMENT AS A MEANS OF FORMATION OF PRACTICAL SKILLS OF STUDENTS SPECIALTY 125 CYBER SECURITY

Abstract. This article examines the problem of implementing active teaching methods for students majoring in 125 Cybersecurity. The study of qualitative analysis of information security risks (IS) is presented on the example of studying the discipline "Risk Theory", namely the use of SWOT-analysis tools for risk assessment in the field of IS of small and medium business. General relevance and possibilities of using SWOT-analysis in the field of IS risk to study the internal environment of the organization, its strengths and weaknesses with the definition of enterprise strategies in the external environment: confronting threats to secure information (confidentiality, availability and integrity), and other its development. Based on scientific sources, the main research of the definition is analyzed: IS risks, risk analysis and their quality assessment. The content and procedure of SWOT-analysis are described. Using forms of group work and active methods (trainings) in the educational process, the basic factors for SWOT-analysis of the virtual organization "Internet Provider" were created, methodical expert assessments were conducted to identify the primary features of these factors, the analysis of the results was obtained.It is proved that the introduction of this technology in the educational process promotes the development of theoretical knowledge and the formation and development of practical skills of future specialists in information and cyber security.

Keywords: information security risks; risk analysis; SWOT analysis; threats; active teaching methods.

REFERENCES (TRANSLATED AND TRANSLITERATED)

[1] The Future of Jobs Report 2020. [Online] Access mode: https://www.weforum.org/reports/the-future-of-jobs-report-2020
[2] S.M. Shevchenko CM Development of analytical thinking of students of higher technical educational institutions in the process of studying mathematical disciplines.- Thesis Cand. Ped. Science: 13.00.02, Nat. Ped. Univ. MP Dragomanova. - K., 2013.- 200 p.
[3] Educational and professional program. 125.00.01. Security of information and communication systems of the first (bachelor's) level of education. B. Hrinchenko University of Kyiv, 2018. [Online] Access mode: http://kubg.edu.ua/images/stories/Departaments/vstupnikam/fitu/2018/2019_bak_op_kiber.pdf

[4] V.L. Buryachok, VM Bogush, Yu.V. Borsukovsky, P.M. Folding, V.Yu. Borsukovska, "Model of training specialists in the field of information and cyber security in higher education institutions of Ukraine", Information technologies and teaching aids, volume 67, №5, p.277-289, 2018.
[5] Buryachok VL, Bogush VM (2018) Recommendations for the development and implementation of a model of professional competencies in the field of training for the national cybersecurity system Information security, Vol. 20 (2). Pp. 72-78. ISSN 2221-5212
[6] Melnyk S., Voskoboynikov S., Stupak D. Organization of professional training of future cybersecurity professionals based on innovative pedagogy and an integrated approach in the system of implementation of key security competencies in the information society. Origins of pedagogical skills, vol. 21, 2018, pp.125 - 129
[7] V. L. Buriachok, S. M. Shevchenko, and P. M. Skladannyi, "Virtual laboratory for process modeling in information and cybersecurity as a means of forming students' practical skills", Cybersecurity: education, science, technology, vol. 2, issue 2, p. 98-104, Dec 2018.
[8] Yu.D. Жданова, C.O. Spasiteleva, SM Shevchenko, "Application of the library of classes Security.Cryptography for practical training of specialists in cybersecurity", Cybersecurity: education, science, technology, 4 (4), p. 44-53, 2019.
[9] Buriachok, Volodymyr and Sokolov, V. Y. (2019) Implementation of Active Learning in the Master's Program on Cybersecurity In: II International Conference on Computer Science, Engineering and Education Applications (ICCSEEA'2019), 26,27 January 2019, Kyiv.
[10] V. Buriachok, N. Korshun, S. Shevchenko, and P. Skladannyi, "Application of the environment ni multisim in the formation of practical skills of students majoring in 125 'cybersecurity'", Cybersecurity: education, science, technology, vol. 1, issue 9, p. 159-169, Sep 2020.
[11] Shevchenko SM, Zhdanova Yu. D., Spasiteleva SO, Adamovich OV Statistical processing of experimental data as one of the forms of research work of students majoring in "Cybersecurity" Modern information protection №2 (30), 2017, p. 95-103
[12] «Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology [Gary Stoneburner, Alice Goguen, Alexis Feringa] », National Institute of Standards and Technology Special Publication 800- 30, Falls Church: Natl. Inst. Stand. Technol, 2002, pp. 54
[13] "Risk analysis based on IT protection", BSI-Standard 100-3, Boon: Bundesamt für Sicherheit in der Informationstechnik, 2008, p. 23
[14] «Information Technology - Security techniques - Information security risk management (ISO / IEC 27005: 2008)», ISO / IEC JTC 1 / SC 27, 2008, p. 62.
[15] DSTU ISO / IEC 27005: 2019 (ISO / IEC 27005: 2018, IDT) "Information technologies. Methods of protection. Information security risk management ", 2019, p. 54
[16] Arkhipov OE, Muratov OE, Brovko VD Fundamentals of risk theory: a textbook - K .: NA SB of Ukraine, 2019. - 267 p.
[17] Akhmetov BB, Korchenko AG, Arkhipov AE, Kazmirchuk SV Construction of information security risk analysis and assessment systems. Theory and practical solutions: monograph (in 2 books) - Aktau: editorial and publishing department of KSUTI. Sh. Esenova, 2018. - 390 p. (book 1), 346 p. (book 2). [Online] Access mode: https://er.nau.edu.ua/handle/nau/40479?locale=uk
[18] Dictionary of systems analysis in public administration. K., 2006, p.148. [Online] Access mode: http://academy.gov.ua/nmkd/library_nadu/encycloped_vydanniy/f4a14404-2b5a-4031-968c-c95c5a50b4c5.pdf
[19] Tim Friesner. History of SWOT Analysis, 2011. [Online] Access mode: https://www.marketingteacher.com/history-of-swot-analysis/
[20] Andrea Berkoff Security SWOT Analysis for 2020: Opportunities, 2020. [Online] Access mode: https://citysecuritymagazine.com/risk-management/security-sector-leaders-swot-analysis-for-2020-opportunities/
[21] Scholarly Commons Citation Baghdasarin, D. (2019). MRO Cybersecurity SWOT. International Journal of Aviation, Aeronautics, and Aerospace, 6 (1). https://doi.org/10.15394/ijaaa.2019.1318
[22] Buryachok, VL Information and cybersecurity: sociotechnical aspect: textbook / [V. L. Buryachok, VB Tolubko, VO Khoroshko, SV Tolyupa]; for general Ed. Dr. Tech. Nauk, profesora VB Tolubka.— K .: DUT, 2015.— 288